UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/690,017	10/21/2003	James P. Goddard	END920030107US1	4833

26502 7590 11/15/2010

IBM CORPORATION
IPLAW SHCB/40-3
1701 NORTH STREET
ENDICOTT, NY 13760

EXAMINER	
HOANG, DANIEL L	
ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
11/15/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

endiplaw@us.ibm.com

Office Action Summary	Application No.	Applicant(s)	
	10/690,017	GODDARD, JAMES P.	
	Examiner	Art Unit	
	DANIEL L. HOANG	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11/13/09*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,7-10,12,15,19 and 25-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,7-10,15,19 and 25-37* is/are rejected.

7)☒ Claim(s) *12* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments, which were discussed in the telephonic interview on 3/22/10 with respect to the rejection(s) of claim(s) 1, 7-10, 15, 19-20, and 25-37 have been fully considered and are persuasive. Applicant contended that the current rejection was insufficient in rejecting the current claim language and that the art applied was not applicable to the claimed invention. Examiner agreed to applicant's claims. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Voss, US Patent No. 7552480.

CLAIMS PRESENTED

Claims 1, 3, 7-10, 12, 15, 19-20, and 25-37 are presented.

CLAIM REJECTIONS

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-3, 7-10, 12, 15, 19-20 are not statutory as they are drawn as a whole to an abstract idea. A review of the factors outlined in the July 27, 2010 policy memo and OG Notice, indicates that these claims are not statutory. These claims fail the machine or transformation test as the steps of a, b and c could be performed in one's mind or manually and involve only the general concept covering both known and unknown uses of the concept covered, and can be performed through any existing or future-devised machinery or even without any apparatus.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 1, 7-10, 15, 19-20, and 25-37 are rejected under 35 U.S.C. 102(e) as being anticipated by Voss, US Patent No. 7552480.

As per claims 1, 25, and 32:

A computer implemented method for evaluating a security risk of an application, said method comprising the steps of:

> *[see col. 3, lines 15-20, "system for assessing and quantifying the risk exposure of an information system or application using a a one-dimensional quantitative risk assessment model.]*

determining whether the application is shared by different customers;

> *[see col. 4, lines 23-32, wherein establishing the numerical value for the threat of attack involves establishing the potential for an attack on the information system asset by a threat agent and further wherein a threat agent is defined as casual users, kiddy scriptors, hackers, disgruntled employees, legitimate consumers, competitors, etc. Examiner understands this to mean that a threat value is calculated based on whether the application can be exploited by different users which is considered to be analogous to applicant's claim language of being shared by different customers.] see also col. 7-8]*

determining whether a third party can have unauthorized administrative authority to data maintained by the application;

> *[see col. 4, lines 42-52, wherein establishing a numerical value includes identifying one or more unauthorized privileges such as security administrator privileges] see also, col. 7-8]*

determining whether a third party can have unauthorized read and/or write access to data maintained by said application;

[see col. 4, lines 42-52, wherein establishing a numerical value includes identifying one or more unauthorized privileges such as super user read privileges.] see also col. 7-8]

assigning a numerical value or weight to each of the foregoing determinations, each of said numerical values or weights corresponding to a significance of the respective determination in evaluating security risk; and combining said numerical values or weights to evaluate security risk.

[see col. 4, lines 53-60, wherein the security risk level for the information asset is calculated as a product of the numerical value of the threat of attack times the numerical value for the access component of the vulnerability times the numerical value for the privilege component of the vulnerability to attack on the information system asset.]

As per claim 7:

A computer implemented method as set forth in claim 1 further comprising the steps of: determining whether a third party can have unauthorized read and write access to said data; and assigning a numerical value or weight to the determination whether a third party can have unauthorized read and write access to said data, and using the numerical value or weight for the determination whether a third party can have unauthorized read and write access to said data in evaluating said security risk.

[see rejection of claim 1]

As per claim 8, 27:

A computer implemented method as set forth in claim 1 further comprising the steps of:
determining whether a vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs; and
assigning a numerical value or weight to the determination whether the vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a

system in which said application runs and using the numerical value or weight for the determination whether a third party can have unauthorized read and write access to said data in evaluating said security risk.

[see col. 8, lines 1-14, wherein Voss teaches that a normal user who exploits a vulnerability might have additional control to see and/or delete other person's data that he or she would not otherwise have]

As per claim 9:

A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether data maintained by or accessed by said application is confidential; and wherein the numerical value or weight assigned to the determination whether a third party can have unauthorized access to said data is based in part on whether said data is confidential.

[see col. 11, unauthorized access to audit logs wherein audit logs are viewed as confidential data]

As per claim 10, 28, 34:

A method as set forth in claim 1 further comprising the steps of:

determining whether a customer has direct use of said application; and assigning a numerical value or weight to the determination whether a customer has direct use of said application, and using the numerical value or weight for the determination whether a customer has direct use of said application in evaluating said security risk.

[see paragraph 8, wherein it is determined whether the vulnerability exists internally or in the form of an external environment]

As per claim 19, 30, 36:

A computer implemented method as set forth in claim 1 further comprising the step of comparing the evaluation of said security risk to a cost savings provided by said application, and determining whether to certify said application for use based in part on said comparison.

[see col. 5, lines 1-16, "monetary value" and "financial impact"]

As per claim 20, 31, 37:

A computer implemented method as set forth in claim 1 further comprising the step of comparing the evaluation of said security risk to a revenue provided by said application, and determining whether to certify said application for use based in part on said comparison.

[see col. 5, lines 1-16, "financial value of the security risk to the entity from attack on the information system asset is calculated based on the financial impact on the entity and the security risk level calculated for the information system."]

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Voss, as applied to claim 1 above, and further in view of Brooks, US PGP No. 20030210139.

As per claim 3:

The Voss reference has been discussed above. While Voss teaches assigning a numerical value to certain security concerns in order to evaluate the security risk, Voss is mute in teaching whether the application is subject to industry controls for security as being a determination from which security risk is evaluated.

For this limitation, examiner relies on the Brooks reference. Brooks teaches a method of evaluating overall security wherein values are compared to existing industry or company standards (see paragraph 9). It would have been obvious to one of ordinary skill in the art to modify the Voss reference in order to include a determination as to whether to application is subject to industry standards as taught by Brooks because an application subject to industry standards is likely to be more secure that one that is not.

3. Claims 15, 29, and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Voss, as applied to claim 1 above, and further in view of Minemura, US PGP No. 20030114144.

As per claim 15, 29, 35:

A computer implemented method as set forth in claim 1 further comprising the steps:
determining whether there is a requirement for authentication of said application or a system in which said application runs to other systems before connection of said application or said system in which said application runs to said other systems; and assigning a numerical value or weight to the determination whether there is a requirement for authentication of said application or a system in which said application runs to other systems before connection of said application or said system in which said application runs to said other systems, and using the numerical value or weight for said requirement for authentication in evaluating said security risk.

Voss has been discussed above. Voss is mute in teaching application authentication as a requirement evaluating security risk. The Minemura reference is relied upon for this limitation.

Minemura teaches an application authentication system (see paragraphs 013-015). It would be obvious to one of ordinary skill in the art to modify the Jones reference to include the application authentication system taught by Minemura because application security is a security risk. It is possible that the

application may be used to perform an invalid operation. Authenticating the application is a possible way of thwarting such attempts. Determining whether the application is required to authenticate would clearly make the system more secure and allow it to better evaluate an application's security risk.

Allowable Subject Matter

4. Claim 12 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

3. Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulaney Street
Alexandria, VA 22314

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Hoang whose telephone number is 571-270-1019. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached at (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-

direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Daniel L. Hoang/
Examiner, Art Unit 2436

/Nasser Moazzami/
Supervisory Patent Examiner, Art Unit 2436